Anomaly Detection Report

Model: autoencoder

Source File: synthetic_logs_test_500_new.csv

Total Anomalies Found: 30

Total Clusters Detected: 3

Detected Attack Clusters

[DoS] - Severity: High | Confidence: 0.90 | Logs: 11

Reasoning: The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Common Pattern: Multiple POST requests with status 500 and high response times to the same destination IP

[Rate limiting anomalies] - Severity: High | Confidence: 0.90 | Logs: 10

Reasoning: The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Common Pattern: The common behavior in this cluster is the repeated use of POST and GET methods for login/authentication endpoints with high response times and zero bytes exchanged.

[Rate limiting anomalies] - Severity: High | Confidence: 0.90 | Logs: 9

Reasoning: The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Common Pattern: The common behavior in this cluster is the repeated POST requests with zero bytes and varying response times.

Anomaly Detection Report

Detailed Anomaly Logs

Anomaly #6 | Severity: High | Type: DoS (Score: 0.3273)

Log Details:

```
syslog_ts: Jan 28 08:10:03 host: servernameabc process: httpd[12345] ip1: 10.21.196.228 ip2: 0.1.0.1 session_id: 26089 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:03 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: 0 response_time: 1904 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #91 | Severity: High | Type: DoS (Score: 0.3452)

Log Details:

```
syslog_ts: Jan 28 08:11:06 host: servernameabc process: httpd[12345] ip1: 10.189.22.211 ip2: 0.1.0.1 session_id: 30038 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:06 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 500 bytes: 0 response_time: 3235 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #155 | Severity: High | Type: DoS (Score: 0.3495)

Log Details:

```
syslog_ts: Jan 28 08:11:58 host: servernameabc process: httpd[12345] ip1: 10.232.226.242 ip2: 0.1.0.1 session_id: 93494 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:58 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: 0 response_time: 3632 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #184 | Severity: High | Type: DoS (Score: 0.3429)

Log Details:

```
syslog_ts: Jan 28 08:12:15 host: servernameabc process: httpd[12345] ip1: 10.10.124.158 ip2: 0.1.0.1 session_id: 11357 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:15 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 503 bytes: 0 response_time: 2739 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

Anomaly Detection Report

(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #258 | Severity: High | Type: DoS (Score: 0.3425)

Log Details:

syslog_ts: Jan 28 08:13:09 host: servernameabc process: httpd[12345] ip1: 10.2.231.200 ip2: 0.1.0.1 session_id: 73898 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:09 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 503 bytes: 0 response_time: 2707 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #336 | Severity: High | Type: DoS (Score: 0.3223)

Log Details:

syslog_ts: Jan 28 08:14:07 host: servernameabc process: httpd[12345] ip1: 10.236.169.131 ip2: 0.1.0.1 session_id: 87520 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:07 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: 0 response_time: 1615 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #357 | Severity: High | Type: DoS (Score: 0.3403)

Log Details:

syslog_ts: Jan 28 08:14:25 host: servernameabc process: httpd[12345] ip1: 10.64.144.18 ip2: 0.1.0.1 session_id: 82377 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:25 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: 0 response_time: 2818 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly Detection Report

Anomaly #371 | Severity: High | Type: DoS (Score: 0.3294)

Log Details:

```
syslog_ts: Jan 28 08:14:36 host: servernameabc process: httpd[12345] ip1: 10.163.35.89 ip2: 0.1.0.1 session_id: 73573 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:36 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: 0 response_time: 2030 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #404 | Severity: High | Type: DoS (Score: 0.3386)

Log Details:

```
syslog_ts: Jan 28 08:15:06 host: servernameabc process: httpd[12345] ip1: 10.241.229.72 ip2: 0.1.0.1 session_id: 46902 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:06 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: 0 response_time: 2680 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #442 | Severity: High | Type: DoS (Score: 0.3508)

Log Details:

```
syslog_ts: Jan 28 08:15:35 host: servernameabc process: httpd[12345] ip1: 10.211.184.25 ip2: 0.1.0.1 session_id: 97333 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:35 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: 0 response_time: 3767 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #446 | Severity: High | Type: DoS (Score: 0.3387)

Log Details:

```
syslog_ts: Jan 28 08:15:37 host: servernameabc process: httpd[12345] ip1: 10.229.48.193 ip2: 0.1.0.1 session_id: 72880 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:37 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: 0 response_time: 2689 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a high number of HTTP requests with status 500 and unusually high response times, indicating a potential Denial of Service (DoS) attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Duration, Method_GET.

Anomaly #52 | Severity: High | Type: Rate limiting anomalies (Score: 0.2155)

Log Details:

```
syslog_ts: Jan 28 08:10:41 host: servernameabc process: httpd[12345] ip1: 10.141.189.59 ip2: 0.1.0.1 session_id: 21976 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:41 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: 0 response_time: 1011 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #80 | Severity: High | Type: Rate limiting anomalies (Score: 0.2382)

Log Details:

```
syslog_ts: Jan 28 08:11:00 host: servernameabc process: httpd[12345] ip1: 10.60.248.68 ip2: 0.1.0.1 session_id: 49119 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:00 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: 0 response_time: 2204 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #81 | Severity: High | Type: Rate limiting anomalies (Score: 0.2292)

Log Details:

```
syslog_ts: Jan 28 08:11:01 host: servernameabc process: httpd[12345] ip1: 10.62.37.180 ip2: 0.1.0.1 session_id: 80667 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:01 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: 0 response_time: 1654 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #119 | Severity: High | Type: Rate limiting anomalies (Score: 0.2322)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:32 host: servernameabc process: httpd[12345] ip1: 10.118.254.130 ip2: 0.1.0.1
session_id: 66698 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:32 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: 0 response_time: 1822 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #242 | Severity: High | Type: Rate limiting anomalies (Score: 0.2389)

Log Details:

```
syslog_ts: Jan 28 08:12:58 host: servernameabc process: httpd[12345] ip1: 10.188.100.99 ip2: 0.1.0.1
session_id: 62599 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:58 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: 0 response_time: 2252 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #294 | Severity: High | Type: Rate limiting anomalies (Score: 0.2532)

Log Details:

```
syslog_ts: Jan 28 08:13:35 host: servernameabc process: httpd[12345] ip1: 10.82.121.215 ip2: 0.1.0.1
session_id: 61632 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:35 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: 0 response_time: 3394 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #365 | Severity: High | Type: Rate limiting anomalies (Score: 0.2591)

Log Details:

```
syslog_ts: Jan 28 08:14:32 host: servernameabc process: httpd[12345] ip1: 10.41.79.10 ip2: 0.1.0.1
session_id: 56871 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:32 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: 0 response_time: 3975 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #373 | Severity: High | Type: Rate limiting anomalies (Score: 0.2347)

Log Details:

syslog_ts: Jan 28 08:14:38 host: servernameabc process: httpd[12345] ip1: 10.59.101.8 ip2: 0.1.0.1 session_id: 86819 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:38 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: 0 response_time: 1972 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #382 | Severity: High | Type: Rate limiting anomalies (Score: 0.2173)

Log Details:

syslog_ts: Jan 28 08:14:46 host: servernameabc process: httpd[12345] ip1: 10.32.209.7 ip2: 0.1.0.1 session_id: 28430 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: 0 response_time: 1087 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #453 | Severity: High | Type: Rate limiting anomalies (Score: 0.2529)

Log Details:

syslog_ts: Jan 28 08:15:45 host: servernameabc process: httpd[12345] ip1: 10.208.102.184 ip2: 0.1.0.1 session_id: 97018 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:45 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: 0 response_time: 3368 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of failed login attempts with a high rate of 1.0, indicating a potential brute force attack or automated login attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Method_POST, Method_GET.

Anomaly #103 | Severity: High | Type: Rate limiting anomalies (Score: 0.1533)

Log Details:

syslog_ts: Jan 28 08:11:18 host: servernameabc process: httpd[12345] ip1: 10.30.253.210 ip2: 0.1.0.1 session_id: 14210 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:18 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: 0 response_time: 1189 referer:

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #151 | Severity: High | Type: Rate limiting anomalies (Score: 0.1650)

Log Details:

syslog_ts: Jan 28 08:11:55 host: servernameabc process: httpd[12345] ip1: 10.91.219.1 ip2: 0.1.0.1 session_id: 94595 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:55 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: 0 response_time: 1779 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #222 | Severity: High | Type: Rate limiting anomalies (Score: 0.1615)

Log Details:

syslog_ts: Jan 28 08:12:45 host: servernameabc process: httpd[12345] ip1: 10.76.83.142 ip2: 0.1.0.1 session_id: 71227 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:45 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: 0 response_time: 1583 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #240 | Severity: High | Type: Rate limiting anomalies (Score: 0.1999)

Log Details:

syslog_ts: Jan 28 08:12:57 host: servernameabc process: httpd[12345] ip1: 10.147.120.32 ip2: 0.1.0.1 session_id: 42237 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:57 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: 0 response_time: 4797 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly Detection Report

Anomaly #343 | Severity: High | Type: Rate limiting anomalies (Score: 0.1949)

Log Details:

```
syslog_ts: Jan 28 08:14:14 host: servernameabc process: httpd[12345] ip1: 10.195.155.50 ip2: 0.1.0.1 session_id: 94099 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: 0 response_time: 4218 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #359 | Severity: High | Type: Rate limiting anomalies (Score: 0.1836)

Log Details:

```
syslog_ts: Jan 28 08:14:28 host: servernameabc process: httpd[12345] ip1: 10.115.140.69 ip2: 0.1.0.1 session_id: 18604 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:28 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: 0 response_time: 3113 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #366 | Severity: High | Type: Rate limiting anomalies (Score: 0.1677)

Log Details:

```
syslog_ts: Jan 28 08:14:33 host: servernameabc process: httpd[12345] ip1: 10.103.133.120 ip2: 0.1.0.1 session_id: 56949 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:33 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: 0 response_time: 1940 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #454 | Severity: High | Type: Rate limiting anomalies (Score: 0.1740)

Log Details:

```
syslog_ts: Jan 28 08:15:46 host: servernameabc process: httpd[12345] ip1: 10.56.72.127 ip2: 0.1.0.1 session_id: 30125 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: 0 response_time: 2355 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.

Anomaly #456 | Severity: High | Type: Rate limiting anomalies (Score: 0.1765)

```
Log Details:
syslog_ts: Jan 28 08:15:46 host: servernameabc process: httpd[12345] ip1: 10.207.201.42 ip2: 0.1.0.1 session_id: 70529 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: 0 response_time: 2536 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of multiple POST requests with zero bytes and varying response times within a short time span, indicating a potential abuse of the server's rate limiting mechanism.

Reason for Detection:

This log is part of an anomaly cluster 'Rate limiting anomalies'. Contributing features: Duration, Size, Method_POST.
